



## Search Results

## BROWSE

## SEARCH

## IEEE Xplore GUIDE

## SUPPORT

Results for "((('s-box' and encryption)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1950 &lt;and&gt; pyr &lt;= 2..."

Your search matched 10 of 1768462 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

 [e-mail](#)  [print this](#)

New [Beta]  
**Application  
Notes**  
IEEE/IEC  
GLOBAL SPEC

## Modify Search


 Check to search only within this results set
Display Format:  Citation  Citation & Abstract
[» Search Options](#)
[View Session History](#)
[New Search](#)

IEEE/IET

Books

Educational Courses

Application Notes [Beta]

IEEE/IET journals, transactions, letters, magazines, conference proceedings, and standards.

 
[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

1. Efficient Rijndael implementation for high-speed optical networks  
 Rejeb, J.; Ramaswamy, V.;  
*Telecommunications, 2003. ITC 2003. 10th International Conference on*  
 Volume 1, 23 Feb.-1 March 2003 Page(s):641 - 645 vol.1  
 Digital Object Identifier 10.1109/ICTEL.2003.1191484  
[AbstractPlus](#) | Full Text: [PDF\(344 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
2. A 10 Gbps full-AES crypto design with a twisted-BDD S-Box architecture  
 Morioka, S.; Satoh, A.;  
*Computer Design: VLSI in Computers and Processors, 2002. Proceedings. 2002 IEEE International Conference on*  
 16-18 Sept. 2002 Page(s):98 - 103  
 Digital Object Identifier 10.1109/ICCD.2002.1106754  
[AbstractPlus](#) | Full Text: [PDF\(1774 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
3. A highly efficient AES cipher chip  
 Chih-Pin Su; Tsung-Fu Lin; Chih-Tsun Huang; Cheng-Wen Wu;  
*Design Automation Conference, 2003. Proceedings of the ASP-DAC 2003. Asia and South Pacific*  
 21-24 Jan. 2003 Page(s):561 - 562  
 Digital Object Identifier 10.1109/ASPDAC.2003.1195078  
[AbstractPlus](#) | Full Text: [PDF\(326 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
4. A high-throughput low-cost AES cipher chip  
 Tsung-Fu Lin; Chih-Pin Su; Chih-Tsun Huang; Cheng-Wen Wu;  
*ASIC, 2002. Proceedings. 2002 IEEE Asia-Pacific Conference on*  
 6-8 Aug. 2002 Page(s):85 - 88  
 Digital Object Identifier 10.1109/APASIC.2002.1031538  
[AbstractPlus](#) | Full Text: [PDF\(337 KB\)](#) [IEEE CNF](#)  
[Rights and Permissions](#)
5. Construction of highly nonlinear injective S-boxes with application to CAST-like encryption algorithms  
 Youssef, A.M.; Chen, Z.G.; Tavares, S.E.;  
*Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on*  
 Volume 1, 25-28 May 1997 Page(s):330 - 333 vol.1  
 Digital Object Identifier 10.1109/CCECE.1997.614856  
[AbstractPlus](#) | Full Text: [PDF\(320 KB\)](#) [IEEE CNF](#)

[Rights and Permissions](#)

6. A high-throughput low-cost AES processor  
Chih-Pin Su; Tsung-Fu Lin; Chih-Tsien Huang; Cheng-Wen Wu;  
*Communications Magazine, IEEE*  
Volume 41, Issue 12, Dec. 2003 Page(s):86 - 91  
Digital Object Identifier 10.1109/MCOM.2003.1252803  
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(515 KB\)](#) | [IEEE JNL](#)  
[Rights and Permissions](#)

7. Hardware implementation of 128-bit symmetric cipher SEED  
Young-Ho Seo; Jong-Hyeon Kim; Dong-Wook Kim;  
*ASICs, 2000. AP-ASIC 2000. Proceedings of the Second IEEE Asia Pacific Conference on*  
28-30 Aug. 2000 Page(s):183 - 186  
Digital Object Identifier 10.1109/APASIC.2000.896939  
[AbstractPlus](#) | [Full Text: PDF\(316 KB\)](#) | [IEEE CFP](#)  
[Rights and Permissions](#)

8. Evaluation of different Rijndael implementations for high end servers  
Mayer, U.; Oelsner, C.; Kohler, T.;  
*Circuits and Systems. 2002. ISCAS 2002. IEEE International Symposium on*  
Volume 2, 26-29 May 2002 Page(s):II-348 - II-351 vol.2  
Digital Object Identifier 10.1109/ISCAS.2002.1010996  
[AbstractPlus](#) | [Full Text: PDF\(406 KB\)](#) | [IEEE CFP](#)  
[Rights and Permissions](#)

9. Large s-box design using a converging method  
Hendessi, F.; Gulliver, T.A.; Sheikh, A.U.H.;  
*Information Theory. 1997. Proceedings., 1997 IEEE International Symposium on*  
29 June-4 July 1997 Page(s):177  
Digital Object Identifier 10.1109/ISIT.1997.613092  
[AbstractPlus](#) | [Full Text: PDF\(132 KB\)](#) | [IEEE CFP](#)  
[Rights and Permissions](#)

10. A new criterion for the design of 8×8 S-boxes in private-key ciphers  
Jianhong Xu; Heys, H.M.;  
*Electrical and Computer Engineering. 1997. IEEE 1997 Canadian Conference on*  
Volume 1, 25-28 May 1997 Page(s):322 - 325 vol.1  
Digital Object Identifier 10.1109/CCECE.1997.614854  
[AbstractPlus](#) | [Full Text: PDF\(316 KB\)](#) | [IEEE CFP](#)  
[Rights and Permissions](#)